

**TECHNIQUES FOR OFFERING SEAMLESS ACCESSES IN ENTERPRISE HOT
SPOTS FOR BOTH GUEST USERS AND LOCAL USERS**

This application claims the benefit, under 35 U.S.C. § 365 of International
5 Application PCT/US04/07065, filed March 8, 2004, which was published in accordance with
PCT Article 21(2) on November 4, 2004 in English and which claims the benefit of United States
provisional patent application No. 60/463,060, filed April 15, 2003.

CROSS-REFERENCE TO RELATED APPLICATIONS

10 This application claims priority under 35 U.S.C. 119(e) to U.S. Provisional Patent
Application Serial No 60/463,060 filed April 15, 2003, the teachings of which are incorporated
herein.

15 **TECHNICAL FIELD**

This invention relates a technique for handling different types of traffic at a wireless
Local Area Network (LAN)

20 **BACKGROUND ART**

Advances in the field of wireless LAN technology has led to the availability of relatively
inexpensive wireless LAN equipment, thus giving rise to the so-called "Enterprise Guesting"
market. Many companies and institutions now offer wireless LAN enterprise access in different
25 locations, such as meeting rooms and lobbies, affording visitors the ability to gain network
access. One key issue associated with Enterprise Guesting is how to distinguish between guests
and internal (i.e., local) users in order to route traffic on different paths. Preferably, guest traffic
should travel to an enterprise gateway for routing to an external destination, such as the Internet
or the guest's own intranet (through VPN). (In the event traffic from a guest is destined for the
30 local network, that traffic should enter the network through a corporate firewall, as would any
other external traffic.) A local user connected via an "Enterprise" access point should receive
wireless access from such an enterprise hot spot just as that user would in other places within the
company having wireless LAN access point(s). Traffic from the local user should enter the local
network just as if the user were connected by a wired connection.

Once existing solution to the problem of separating local user traffic from guest traffic requires that only guests enjoy wireless LAN access at an enterprise access point ("hot spot".) Local users must access the enterprise access point just like visitors do. To allow a local user to enjoy access to the local intranet, one or more additional access points must exist alongside enterprise (guest host) access point(s). Another solution makes use of MAC addresses to distinguish between guests and local users. Such a solution requires all local users to register their wireless cards and requires maintenance of a hardware database.

Thus, there is need for a technique for separating traffic from guests and local users at an enterprise hot spot that overcomes the aforementioned disadvantages.

BRIEF SUMMARY OF THE INVENTION

Briefly, in accordance with a preferred embodiment of the present principles, there is provided a method for offering wireless LAN access to both local users (i.e., parties that are known to the wireless LAN) as well as guests, (i.e., parties typically unknown to the wireless LAN). The method commences upon receipt of a request for access at an access point in the wireless LAN capable of accommodating both local users and guests. The party requesting access undergoes authentication in accordance with that party's status (that is, whether the party is a local user or guest). In other words, to the extent that no determination has been made prior to authentication as to the status of the party seeking access, the authentication server will determine the status of the party. Upon successful authentication, different routing occurs for the traffic from a local user as compared to that for a guest. For example traffic from guests goes to gateway for receipt in an external network such as the Internet, whereas traffic from the local user goes to a local network, e.g., a corporate intranet. In this way, the Wireless LAN, after ascertaining the status of the party requesting access, can limit guest traffic according to the guest access policy.

BRIEF DESCRIPTION OF THE DRAWING

FIGURE 1 depicts a block schematic diagram of an enterprise guest host architecture in accordance with a preferred embodiment of the present principles.

DETAILED DESCRIPTION

FIGURE 1 depicts an enterprise guest host architecture 10 that includes a wireless Local Area Network (LAN) 11 for offering seamless wireless access to both a guest user 12 and a local user 14 through an enterprise-guesting Access Point (AP) 15 that can accommodate both local users and guests. For purposes of discussion, the guest user 12 constitutes a party that has no service relationship with the wireless LAN 11, i.e., the party isn't registered with the wireless LAN and thus lacks the same privileges of a local user 14. Although FIG. 1 depicts a single guest 12 and single local user 14, additional guests and/or users can access the access point 15 or other such access points (not shown) in accordance with the present principles.

For security reasons, traffic from guests should remain segregated from the traffic of local users. In other words, each guest 12 should not have the same privileges as each local user 14. Such local privileges could include access via a corporate intranet 16 to one or more intranet applications residing on a server 17. In the past, segregation of traffic between guests and local users necessitated the use of separate access points. In other words, each guest user 12 would access a guest user access point (not shown), whereas each local user would need to access the wireless LAN 11 through a normal (i.e., local user) access point, such as access point 18, to enjoy the privileges of a local user. Under such an arrangement, a guest could not access the normal access point 18.

In accordance the present principles, there is provided a technique offering wireless LAN access to both guests and local users that segregates the traffic as between guests and local users while allowing both parties to gain wireless LAN access without the need for separate access points. In other words, both the guest 12 and local user 14 can access the wireless LAN 11 through the access point 15, but only the local user 14 accessing that access point can enjoy the privileges of a local user, including gaining access to the server 17. The guest 12 only has access to the intranet 16 for the purpose of communicating with an external network, such as the Intranet 19, with such access made through a corporate firewall 20. The present technique makes use of the intelligence in the Wireless LAN 11, and more specifically, the intelligence in the access point 15, to screen guests 12 from local users 14.

As discussed, the access point 15 has the capability to accommodate the different parties seeking wireless LAN access. To that end, the access point 15 has the capability to select the best authentication method for each party. For example, the access point 15 can determine whether a party seeking access has the ability to employ the IEEE 802.1x protocol. If so, the access point 15 initiates authentication based on the IEEE 802.1x protocol. Otherwise, the access

point 15 initiates web browser based authentication. Based on the authentication result, access point 15 determines whether the party seeking access constitutes a local user 14 or a guest 12, and routes the traffic accordingly. Each local user 14 undergoes authentication differently than each guest 12. Such different authentication can occur via different backend servers (not shown) or by a single authentication server, such as authentication proxy 18 but with different user credentials for each local user 14 and guest 12.

To better appreciate the manner in which such separate authentication occurs, consider the access arrangement depicted in FIG. 1. Each guest 12 typically receives special guest access credentials in advance of seeking access to the wireless LAN 11. Such credentials can comprise combination of a user name and a password, or simply an access key. All the guests can share a common credential, or each guest can receive a credential unique to that guest. All guest credentials share a common criterion, namely, that such credentials only permit guest accesses.

Various techniques exist which allow guests to use their credentials to authenticate themselves. For example, each guest 12 could configure his/her IEEE 802.1x client with a guest credential. Alternatively, each guest 12 could let the access point 15 initiate web browser- based authentication. Each such technique is described below in greater detail

IEEE 802.1x Authentication

Under this scenario, the guest 12 configures his/her IEEE 802.1x client with the guest credential and then commences authentication process. Upon receipt of a request for guest authentication using the IEEE 802.1x protocol, the access point 15 communicates with a backend authentication server, such as authentication proxy 21, using a protocol such as the RADIUS protocol. At least two possible ways exist for the access point 15 to distinguish between guests and local users. For example, the access point 15 could possess the ability to communicate with multiple authentication servers (not shown). A guest would configures his/her IEEE 802.1x user name with a domain name (in the form of user_name@domain_name) where domain_name is special and only has local meaning, e.g. "guest_access". Regular local intranet users keep their normal user name format, i.e. just the user name without the domain name. On this basis, the access point 15 could easily differentiate between guests and local users, and forward authentication traffic from the guest 12 to the proper authentication server, such as authentication proxy 21. The access point 15 can directly determine the guest 12 from his/her domain_name without help from the backend server (i.e., authentication proxy 21). Thus no backend server

changes are necessary. After successful authentication, the access point 15 can route the user traffic accordingly.

As shown in FIG. 1, the access point 15 communicates with a single authentication server, in the form of authentication proxy 21. Each Guest configures his/her IEEE 802.1x user name in the normal format. The access point 15 forwards all IEEE 802.1x authentication traffic to the authentication proxy 21, which has authentication responsibility. Upon successful authentication, the authentication proxy 21 notifies the access point 15 regarding the success or failure of authentication. The access point 15 can then route the user traffic accordingly.

10 Web browser based authentication

In the case that a party seeking access does not have an IEEE 802.1x client or has difficulty understanding the configuration process, he or she can choose to employ a user-friendly web browser based authentication technique. Under such circumstances, the access point 15 provides the party seeking access with a welcome page listing various available authentication options. On the welcome page will appear different options, allowing the party seeking access to identify itself as either a guest or local user. The party will select the appropriate option, leading to subsequent authentication. The access point 15 thus can determine whether the party seeking access either is a local user or guest the user based on the party's initial identification.

As described thus far, the determination of whether the party seeking access constitutes a local user or a guest precedes the authentication process. Such a determination need not always precede authentication. For example, it is possible that both guest and local users could use the same configuration (e.g. without a domain). Under such circumstances, the authentication proxy 21 would differentiate between these two types of users by checking a user database (not shown) that would specifically designate guests.

Null Authentication

The wireless LAN 11 could offer an option that would obviate the need for authentication of guests. Under certain circumstances, the wireless LAN 11 could choose not to inconvenience the guest users with special credentials and the login process. Such a decision assumes that those seeking access are sufficiently trustworthy and little if any abuse of the access point 15 would

occur (e.g., the wireless signal generated by the access point has a limited coverage and can be contained within the building). In such a case, the access point 15 only needs to distinguish between guests, who require no authentication, and local users that can pass through with authentication. This scenario incurs the difficulty that the guest traffic will not undergo encryption and those accessing the access point 15 hot spot can see all of the traffic. The problem is not necessary critical since most guests 12 connect to their home networks (not shown) through Virtual Private Network (VPN) software and the traffic will be protected by the VPN tunnel.

The foregoing describes a technique for offering wireless LAN access to both guests and local users at a single access point.